

A New Hybrid Algorithm for Computing a Fast Discrete Fourier Transform

I. S. Reed

University of Southern California

T. K. Truong

Tracking and Data Acquisition Engineering

For certain long transform lengths, Winograd's algorithm for computing the discrete Fourier transform (DFT) is extended considerably. This is accomplished by performing the cyclic convolution, required by Winograd's method, with the Mersenne-prime number-theoretic transform developed originally by Rader. This new algorithm requires fewer multiplications than either the standard fast Fourier transform (FFT) or Winograd's more conventional algorithm.

I. Introduction

Several authors (Refs. 1 through 13) have shown that transforms over finite fields or rings can be used to compute circular convolutions without round-off error. Recently, Winograd (Ref. 14) developed a new class of algorithms which depend heavily on the computation of a cyclic convolution for computing the conventional DFT. This new algorithm, for a few hundred transform points, requires substantially fewer multiplications than the conventional FFT algorithm.

C. M. Rader (Ref. 3) defined a special class of finite Fourier-like transforms over $GF(q)$, where $q = 2^p - 1$ is a Mersenne prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, \dots$. These number-theoretic transforms are used and specialized here to transform lengths of p points. The advantage of this transform over others is that it can be accomplished simply by circular shifts, i.e., no multiplications are needed (Ref. 3).

In this paper, it is shown that Winograd's algorithm can be combined with the above-mentioned number-theoretic trans-

form over $GF(q)$ to yield a new algorithm for computing the discrete Fourier transform (DFT). By this means, a fast method for accurately computing the DFT of a sequence of real and complex numbers of very long transform lengths is obtained.

II. Cyclic Convolution

The following algorithm for the cyclic convolution of two sequences is based on ideas due to Winograd (Ref. 14). Let R be the field of rationals. Also let $X(u) = x_0 + x_1u + x_2u^2 + \dots + x_nu^{n-1}$, $Y(u) = y_0 + y_1u + y_2u^2 + \dots + y_nu^{n-1}$ be two polynomials over R . The product $T(u) = X(u) \cdot Y(u)$ can be computed by

$$T(u) = X(u) \cdot Y(u) \bmod \prod_{i=0}^{2n-2} (u - \alpha_i) \quad (1)$$

where $\alpha_i \in R$. It is shown in (Ref. 14) that a minimum of $2n - 1$ multiplications are needed to compute Eq. (1).

It is readily shown that the cyclic convolution of $X(u)$ and $Y(u)$ is the set of coefficients of the polynomial,

$$T(u) = X(u) \cdot Y(u) \bmod (u^n - 1)$$

Let the polynomial $u^n - 1$ be factored into irreducible relatively prime factors, i.e.,

$$u^n - 1 = \prod_{i=1}^k g_i(u)$$

where

$$(g_i(u), g_j(u)) \neq 1 \text{ for } i \neq j$$

Then $T(u) \bmod g_i(u)$ for $i = 1, 2, \dots, k$ can be computed, using Eq. (1). Finally, the Chinese remainder theorem is used to evaluate $T(u)$ from these residues. The above summarizes Winograd's method for performing a cyclic convolution.

The following theorem, due to Winograd (Ref. 15), will be needed.

Theorem 1: Let a and b be relatively prime positive integers and \mathbf{A} be the cyclic $ab \times ab$ matrix, given by

$$\mathbf{A}(x, y) = f(x + y \bmod a \cdot b), 0 \leq x, y < ab$$

If π is a permutation of the set of integers $\{0, 1, \dots, ab - 1\}$, let

$$\mathbf{B}(x, y) = \mathbf{A}(\pi(x), \pi(y))$$

Then there exists a permutation π such that, if \mathbf{B} is partitioned into $b \times b$ submatrices, each submatrix is cyclic and the submatrices form an $a \times a$ cyclic matrix.

It was shown in (Refs. 15 and 16) that the number of multiplications needed to perform a circular convolution of 2, 3, 4, 5, 6, and 8 points is 2, 4, 5, 10, 8, and 14 multiplications, respectively. To compute the cyclic convolution of two longer sequences of integers, a p -point transform over $GF(q)$ will be utilized here. Since the latter transform can be evaluated without multiplications (Ref. 3), it can be used with considerable advantage to compute the cyclic convolution of two

p -point real number sequences. Hence, for the transform over $GF(q)$, the number of integer multiplications needed to perform a circular convolution is precisely p , excluding the multiplications by p^{-1} in the inverse transform.

III. The DFT When the Transform Length d is a Prime $d = q'$

The DFT is defined by

$$A_j = \sum_{i=0}^{d-1} a_i w^{ij}$$

where w is a d -th root of unity. Let

$$A_0 = \sum_{i=0}^{d-1} a_i \quad (2a)$$

and

$$A_j = a_0 + B_j \text{ for } j = 1, 2, \dots, d-1$$

where

$$B_j = \sum_{i=1}^{d-1} a_i w^{ij}$$

That is, let

$$\bar{\mathbf{B}} = \mathbf{W} \bar{\mathbf{a}} \quad (2b)$$

where \mathbf{W} is the $(d-1) \times (d-1)$ matrix (w^{ij}) , and $\bar{\mathbf{a}}, \bar{\mathbf{B}}$ are the column matrices (a_i) and (B_k) , respectively. If $d = q'$ is a prime, then by (Ref. 13), one can find an element α in $GF(q')$ that generates its cyclic multiplicative subgroup of $q' - 1$ elements. Using the element α , a cyclic permutation of the elements of $GF(q')$ can be defined by

$$\sigma = \begin{pmatrix} 1, 2, \dots, q' - 2, q' - 1 \\ \alpha, \alpha^2, \dots, \alpha^{q'-2}, \alpha^{q'-1} \end{pmatrix} \quad (2c)$$

With this permutation, one can permute the indices of $\bar{\mathbf{B}}, \bar{\mathbf{a}}, \mathbf{W}$ defined in Eq. (2b) so that the matrix $\tilde{\mathbf{W}} = (w^{\sigma(i)\sigma(j)})_{i,j=0}$ is cyclic. That is,

$$\begin{aligned} B_{\sigma(j)} &= \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\sigma(i)\sigma(j)} \\ &= \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\alpha^{i+j}} \\ &= \sum_{i=1}^{q'-1} a_{\sigma(i)} w^{\sigma(i+j)} \quad \text{for } j = 1, 2, \dots, q' - 1 \end{aligned} \quad (3)$$

Thus, $B_{\sigma(j)}$ is a cyclic convolution of $a_{\sigma(i)}$ and $w^{\sigma(i)}$ for $j = 1, 2, \dots, q' - 1$.

Let $q' - 1 = p_1 \cdot p_2 \cdots p_r$, where $(p_i, p_j) = 1$ for $i \neq j$. If one lets $a_1 = p_1 \cdot p_2 \cdots p_{r-1}$ and $b_1 = p_r$, by Theorem 1 the cyclic matrix \mathbf{W} can be partitioned into $b_1^2 = p_r^2$ cyclic matrices each of block size $a_1 \times a_1$. Next let $a_1 = a_2 \times b_2$, where $a_2 = p_1 \cdots p_{r-2}$ and $b_2 = p_{r-1}$. If a_2 is not a prime, then each $a_1 \times a_1$ cyclic matrix can be partitioned into b_2^2 cyclic matrices of block size $a_2 \times a_2$. In general, $a_i = a_{i+1} \cdot b_{i+1}$, where b_{i+1}^2 is a prime. If $a_{i+1} \neq 1$, then each $a_i \times a_i$ cyclic matrix can be partitioned into b_{i+1}^2 cyclic matrices of block size $a_{i+1} \times a_{i+1}$. Otherwise, the procedure terminates. If the number of multiplications used to compute the cyclic con-

volution of p_i points is m_i for $i = 1, 2, \dots, r$, then Winograd has shown in Ref. 14 that the number of multiplications for computing a q' -point DFT is equal to $N = m_1 \cdot m_2 \cdots m_r$.

For most applications, the two Mersenne primes $2^{31} - 1$ and $2^{61} - 1$ will provide enough bit accuracy and dynamic range for computing the DFT. For these primes, we choose the prime q' to have the form

$$q' = 1 + (a \cdot 2^n) \cdot p \quad \text{for } n = 1, 2, 3$$

where $p = 31$ or 61 and $a = 3$ or 5 . Such values for the prime q' are 367, 373, 733, 1831, 1861, and 2441.

If $d = q'$ is the transform length of the DFT, then, by Theorem 1, there exists a permutation of rows and columns so that cyclic matrix \mathbf{W} can be partitioned into blocks of $p \times p$ cyclic matrices, such that the blocks from a $(2^n \cdot a) \times (2^n \cdot a)$ cyclic matrix. This cyclic matrix can be reduced further by Winograd's method. First $q' - 1 = 2^n \cdot a \cdot p$ is an even number, and $w^{2^n \cdot ap} = w^{-1}$ where w is the d -th root of unity in the field of complex numbers. For such a case, Winograd showed that the elements in the $p \times p$ cyclic matrices finally required by the transform are either all real or imaginary numbers. To show this, consider the case $n = 1$. For this case, $q' - 1 = 2 \cdot a \cdot p$. The permutation in Eq. (2c) is given by

$$\sigma = \begin{pmatrix} 1, 2 \cdots ap - 1, ap, ap + 1 \cdots 2ap \\ \alpha, \alpha^2 \cdots \alpha^{ap-1}, \alpha^{ap}, \alpha^{ap+1} \cdots \alpha^{2ap} \end{pmatrix}$$

where α is a generator of the multiplicative subgroup consisting of $q' - 1 = 2ap$ elements in $GF(q')$. Applying the above permutation to Eq. (2b) and using the fact that $\alpha^{ap} \equiv -1 \pmod{q'}$, one obtains the cyclic matrix equation in terms of w as follows:

$$\begin{bmatrix} b_{\sigma(1)} \\ b_{\sigma(2)} \\ \vdots \\ b_{\sigma(2ap)} \end{bmatrix} = \begin{bmatrix} w^{\alpha^2} w^{\alpha^3} w^{\alpha^4} \cdots w^{-1} w^{-\alpha} w^{-\alpha^2} \cdots w^1 w^{\alpha} \\ w^{\alpha^3} w^{\alpha^4} \cdots w^{-1} w^{-\alpha} w^{-\alpha^2} \cdots w^1 w^{\alpha} w^{\alpha^2} \\ \vdots \\ w^{\alpha^1} w^{\alpha^2} \cdots w^{-1} w^{-\alpha} \cdots w^1 \end{bmatrix} \begin{bmatrix} a_{\sigma(1)} \\ a_{\sigma(2)} \\ \vdots \\ a_{\sigma(2ap)} \end{bmatrix} \quad (4)$$

Let $\varphi_0 = b_{\sigma(1)}, \varphi_1 = b_{\sigma(2)}, \dots, \varphi_{2ap-1} = b_{\sigma(2ap)}, x_0 = w^{\alpha^1}, x_1 = w^{\alpha^2}, \dots, x_{ap} = w^{-1}, \dots, x_{2ap} = w^1, y_0 = a_{\sigma(1)}, y_1 = a_{\sigma(2)}, \dots, y_{2ap-1} = a_{\sigma(2ap)}$. Then Eq. (4) becomes

$$\begin{bmatrix} \varphi_0 \\ \varphi_1 \\ \vdots \\ \varphi_{m-2} \\ \varphi_{m-1} \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \cdots & x_{m/2} & \cdots & x_m & x_0 \\ x_2 & x_3 & \cdots & x_{m/2+1} & \cdots & x_0 & x_1 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ x_m & x_0 & x_1 & \cdots & x_{m/2-1} & \cdots & x_{m-1} \\ x_0 & x_1 & x_2 & \cdots & x_{m/2} & \cdots & x_m \end{bmatrix} \begin{bmatrix} y_0 \\ \vdots \\ y_{m-1} \end{bmatrix} \quad (5)$$

where $m = 2ap$.

By Theorem 1, the above cyclic $2 \times ap$ matrix equation can be partitioned into blocks of $ap \times ap$ cyclic matrices, so that the blocks form a 2×2 cyclic matrix. To illustrate this, note first that 2 and $a \cdot p$ are relatively prime. Thus, the Chinese remainder theorem, an isomorphism

$$k \rightarrow (k_1, k_2)$$

exists between an integer k modulo m and the pairs of integers k_1 and k_2 modulo 2 and $a \cdot p$, respectively. This relationship between k and (k_1, k_2) is

$$k = k_1 M_1^{-1} + k_2 M_2^{-1} \pmod{m}$$

where M_1^{-1} and M_2^{-1} satisfy the congruences $a \cdot p M_1^{-1} \equiv 1 \pmod{2}$ and $2 M_2^{-1} \equiv 1 \pmod{a \cdot p}$, respectively.

Let the variables $y_k = y_{(k_1, k_2)}$, $x_k = x_{(k_1, k_2)}$ and $\varphi_k = \varphi_{(k_1, k_2)}$ be rearranged in such a manner that when the first component k of the index pair (k_1, k_2) is 0, component k_2 is in ascending order, and when component k_1 is set to 1, component k_2 also is in ascending order. The variables $x_{(k_1, k_2)}$ for Eq. (5) are then rearranged in the order

$$x_{(0,0)}, x_{(0,1)}, x_{(0,2)}, \dots, x_{(0,ap-1)}, x_{(1,0)}, x_{(1,1)}, x_{(1,2)}, \dots, x_{(1,ap-1)}$$

If such a rearrangement is made also on the variables y_k, x_k , and φ_k , respectively, the cyclic convolution of Eq. (5) has the form

$$\begin{bmatrix} \varphi_{(0,0)} \\ \varphi_{(0,1)} \\ \vdots \\ \varphi_{(0,ap-1)} \\ \varphi_{(1,0)} \\ \vdots \\ \varphi_{(1,ap-1)} \end{bmatrix} = \begin{bmatrix} x_{(1,1)}, x_{(1,2)} \cdots, x_{(1,0)}, x_{(0,1)}, x_{(0,2)} \cdots x_{(0,0)} \\ \vdots \\ x_{(1,ap-1)}, x_{(1,0)} \cdots x_{(1,ap-2)}, x_{(0,ap-1)}, x_{(0,0)} \cdots x_{(0,ap-2)} \\ x_{(1,0)} \quad x_{(1,1)} \cdots x_{(1,ap-1)}, x_{(0,0)} \quad x_{(0,1)} \cdots x_{(0,ap-1)} \\ x_{(0,1)} \quad x_{(0,2)} \cdots x_{(0,0)} \quad x_{(1,1)} \quad x_{(1,2)} \cdots x_{(1,0)} \\ \vdots \\ x_{(0,ap-1)}, x_{(0,0)} \cdots x_{(0,ap-2)}, x_{(1,ap-1)}, x_{(1,0)} \cdots x_{(1,ap-2)} \\ x_{(0,0)} \quad x_{(0,1)} \cdots x_{(0,ap-1)}, x_{(1,0)} \quad x_{(1,1)} \cdots x_{(1,ap-1)} \end{bmatrix} \begin{bmatrix} y_{(0,0)} \\ y_{(0,1)} \\ \vdots \\ y_{(0,ap-1)} \\ y_{(1,0)} \\ \vdots \\ y_{(1,ap-1)} \end{bmatrix} \quad (6)$$

Observe that the matrix Eq. (6) can be further reduced to block form as follows

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} A & B \\ B & A \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \quad (7)$$

where

$$x_1 = \begin{bmatrix} \varphi_{(0,0)} \\ \varphi_{(0,1)} \\ \vdots \\ \varphi_{(0,ap-1)} \end{bmatrix}, \quad x_2 = \begin{bmatrix} \varphi_{(1,0)} \\ \varphi_{(1,1)} \\ \vdots \\ \varphi_{(1,ap-1)} \end{bmatrix}$$

$$\mathbf{y}_1 = \begin{bmatrix} y_{(0,0)} \\ y_{(0,1)} \\ \cdot \\ \cdot \\ \cdot \\ y_{(0,ap-1)} \end{bmatrix}, \quad \mathbf{y}_2 = \begin{bmatrix} y_{(1,0)} \\ y_{(1,1)} \\ \cdot \\ \cdot \\ \cdot \\ y_{(1,ap-1)} \end{bmatrix}$$

$$\mathbf{A} = \begin{bmatrix} x_{(1,1)} & x_{(1,2)} & \cdots & x_{(1,0)} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ x_{(1,ap-1)}x_{(1,0)} & \cdots & x_{(1,ap-2)} \\ x_{(1,0)} & x_{(1,1)} & \cdots & x_{(1,ap-1)} \end{bmatrix}$$

and

$$\mathbf{B} = \begin{bmatrix} x_{(0,1)} & x_{(0,2)} & \cdots & x_{(0,0)} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ x_{(0,ap-1)}x_{(0,0)} & \cdots & x_{(0,ap-2)} \\ x_{(0,0)} & x_{(0,1)} & \cdots & x_{(0,ap-1)} \end{bmatrix}$$

Since

$$x_{(0,ap-1)} = w^{\alpha^{(0,ap-1)+(1,1)}} = w^{\alpha^{(1,0)}} = w^{-1}$$

then

$$\begin{aligned} x_{(1,j)} &= w^{\alpha(1,j)+(1,1)} = w^{\alpha(0,j+1)} = w^{\alpha(1,0)+(1,j+1)} \\ &= w^{-\alpha(1,j+1)} = w^{-\alpha(0,j)+(1,1)} = x_{(0,j)}^* \end{aligned}$$

for $j = 0, 1, \dots, ap - 1$ where $*$ denotes complex conjugation. Thus, in (7), the cyclic matrix \mathbf{A} is the complex conjugate of the cyclic matrix \mathbf{B} , i.e.,

$$\mathbf{A} = \mathbf{B}^* \quad (8)$$

The matrix Eq. (7) can be obtained by computing the set of coefficients of

$$T(u) \equiv (\mathbf{B} + Au) \cdot (y_2 + y_1 u) \bmod (u^2 - 1) \quad (9)$$

where $u^2 - 1 \equiv (u - 1)(u + 1)$ and $u - 1$ and $u + 1$ are relatively prime polynomials.

Taking the congruences of $T(u)$ in Eq. (9) modulo $u - 1$ and $u + 1$, respectively,

$$T_1(u) \equiv (\mathbf{B} + \mathbf{A}) \cdot (y_2 + y_1) \bmod u - 1 \quad (10a)$$

and

$$T_2(u) \equiv (\mathbf{B} - \mathbf{A}) \cdot (y_2 - y_1) \bmod u + 1 \quad (10b)$$

By the Chinese remainder theorem, $T(u)$ can be reconstituted from Eqs. (10a) and (10b) as follows:

$$\begin{aligned} T(u) &= 2^{-1} [(\mathbf{B} + \mathbf{A}) \cdot (y_2 + y_1) - (\mathbf{B} - \mathbf{A}) \cdot (y_2 - y_1) \\ &\quad + ((\mathbf{B} + \mathbf{A}) \cdot (y_2 + y_1) + (\mathbf{B} - \mathbf{A}) \cdot (y_2 - y_1)) u] \\ &= \mathbf{x}_1 + \mathbf{x}_2 u \end{aligned}$$

This is reexpressed in matrix form as

$$\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} (\mathbf{B} + \mathbf{A}) \cdot (y_2 + y_1) + (\mathbf{A} - \mathbf{B}) \cdot (y_2 - y_1) \\ (\mathbf{A} + \mathbf{B}) \cdot (y_2 + y_1) - (\mathbf{A} - \mathbf{B}) \cdot (y_2 - y_1) \end{bmatrix} \quad (11)$$

By Eq. (8), the elements of the cyclic matrices $(\mathbf{B} + \mathbf{A})$ and $(\mathbf{A} - \mathbf{B})$ in Eq. (11) are evidently real and imaginary numbers. Since $(a, p) = 1$, again by Theorem 1, the cyclic matrices $(\mathbf{B} + \mathbf{A})$ and $(\mathbf{A} - \mathbf{B})$ can be partitioned into blocks of $p \times p$ cyclic matrices such that the blocks are $a \times a$ cyclic matrices. Thus, the elements of these $p \times p$ cyclic matrix blocks are either real numbers or imaginary numbers, never complex numbers. Hence, if the input datum is real, then a multiplication by an element in such a $p \times p$ cyclic matrix requires only one real multiplication. If the input datum is a complex number, then a multiplication by an element in such a $p \times p$ cyclic matrix requires two real multiplications.

Using a procedure precisely similar to that used above for $n = 1$, it can be shown that the elements in the required $p \times p$ cyclic matrices of the $2^n \cdot ap$ cyclic matrix for $n = 2, 3$ are also either real numbers or imaginary numbers. It was pointed out in the last section that a transform of length p over $GF(q)$ can be used to compute the cyclic convolution of p real number points. The number of multiplications needed to perform this convolution is p . If one combines this with the number of multiplications needed for Winograd's algorithm for the prime q' , the total number of multiplications required to perform a DFT of $d = q'$ real or complex number points can be computed. The results are shown in Table 1.

It has been shown that Winograd's algorithm can be combined with a transform over $GF(q)$ to yield a new rather fast hybrid algorithm for computing the DFT of real and complex values. In this algorithm, it is necessary to compute the cyclic convolution of p real number points. This cyclic convolution of two p -point sequences of real number points is given by

$$c_k = \sum_{n=0}^{p-1} e_n f_{(k-n)} \quad \text{for } k = 0, 1, 2, \dots, p-1 \quad (12)$$

where $c_k, e_n, f_n \in GF(q)$ and $(k-n)$ denotes the residue of $k-n$ mod p . To compute this convolution, the components of the truncated real number e_n and f_n must be converted first to integers a_n and b_n with dynamic ranges, A and B , respectively. In Refs. 6 and 9, it was shown that a sufficient dynamic range constraint for A and B is

$$A \leq \frac{q-1}{2Bp} \quad (13a)$$

If $A = B$, Eq. (13a) reduces to

$$A \leq \left\lceil \sqrt{\frac{q-1}{2p}} \right\rceil \quad (13b)$$

where $\lceil x \rceil$ denotes the greatest integer less than x .

If the circular convolution of a_n and b_n is denoted by c'_k for $k = 0, 1, 2, \dots, p-1$, then, using the procedure described in the example of Ref. 7, c'_k can be obtained by using fast transforms over $GF(q)$. c_k in Eq. (12) can be obtained by scaling back c'_k to the scale of the original real numbers for $k = 0, 1, 2, \dots, p-1$. Evidently, the only error made in this computation of c'_k is the truncation error.

The dynamic range constraint, A , of the input sequence given in Eq. (13b) is generally very pessimistic. It was shown in Ref. 17 that for integer convolutions, one can lessen the severity of the dynamic range constraint (13) and still maintain c_k in the interval $\pm(q-1)/2$ with a small probability of overflow.

To illustrate this new hybrid algorithm, consider the following example.

Example: Consider the DFT for $d = 7$ points. Let the input function be defined by

$$\begin{aligned} a_n &= 1 \quad \text{for } n = 0, 2 \\ &= 0 \quad \text{for } n = 1, 3, 4, 5, 6 \end{aligned}$$

By Eq. (2a), this transform is

$$A_0 = \sum_{i=0}^6 a_i = 2 + \hat{i} 0 \quad (14a)$$

and

$$A_j = a_0 + b_j \quad \text{for } j = 1, 2, \dots, 6 \quad (14b)$$

where

$$b_j = \sum_{i=1}^{6-1} a_i w^{ij}, \quad w = e^{i2\pi/7}$$

For $d = 7$, the permutation σ is given by

$$\sigma = \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6 \\ 3, & 2, & 6, & 4, & 5, & 1 \end{pmatrix}$$

Applying the above permutation to Eq. (14b), one obtains $\bar{\mathbf{B}} = \bar{\mathbf{W}} \bar{\mathbf{a}}$ as

$$\begin{pmatrix} b_3 \\ b_2 \\ b_6 \\ b_4 \\ b_5 \\ b_1 \end{pmatrix} = \begin{pmatrix} w^2 & w^6 & w^4 & w^5 & w^1 & w^3 \\ w^6 & w^4 & w^5 & w^1 & w^3 & w^2 \\ w^4 & w^5 & w^1 & w^3 & w^2 & w^6 \\ w^5 & w^1 & w^3 & w^2 & w^6 & w^4 \\ w^1 & w^3 & w^2 & w^6 & w^4 & w^5 \\ w^3 & w^2 & w^6 & w^4 & w^5 & w^1 \end{pmatrix} \begin{pmatrix} a_3 \\ a_2 \\ a_6 \\ a_4 \\ a_5 \\ a_1 \end{pmatrix}$$

By Theorem 1, there exists a permutation π of rows and columns so that the above cyclic matrix can be partitioned into 2×2 block matrix of 3×3 cyclic blocks as follows:

$$\begin{pmatrix} b_3 \\ b_5 \\ b_6 \\ b_4 \\ b_2 \\ b_1 \end{pmatrix} = \begin{pmatrix} w^2 & w^1 & w^4 & w^5 & w^6 & w^3 \\ w^1 & w^4 & w^2 & w^6 & w^3 & w^5 \\ w^4 & w^2 & w^1 & w^3 & w^5 & w^6 \\ w^5 & w^6 & w^3 & w^2 & w^1 & w^4 \\ w^6 & w^3 & w^5 & w^1 & w^4 & w^2 \\ w^3 & w^5 & w^6 & w^4 & w^2 & w^1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad (15)$$

This matrix equation has the block form,

$$\begin{aligned} \begin{pmatrix} \mathbf{B}_1 \\ \mathbf{B}_2 \end{pmatrix} &= \begin{pmatrix} \mathbf{C} & \mathbf{D} \\ \mathbf{D} & \mathbf{C} \end{pmatrix} \begin{pmatrix} \mathbf{Z}_1 \\ \mathbf{Z}_2 \end{pmatrix} \\ &= 2^{-1} \begin{pmatrix} (\mathbf{C} + \mathbf{D})(\mathbf{Z}_1 + \mathbf{Z}_2) + (\mathbf{C} - \mathbf{D})(\mathbf{Z}_1 - \mathbf{Z}_2) \\ (\mathbf{C} + \mathbf{D})(\mathbf{Z}_1 + \mathbf{Z}_2) - (\mathbf{C} - \mathbf{D})(\mathbf{Z}_1 - \mathbf{Z}_2) \end{pmatrix} \\ &= 2^{-1} \begin{pmatrix} \mathbf{E} + \mathbf{F} \\ \mathbf{E} - \mathbf{F} \end{pmatrix} \end{aligned} \quad (16)$$

Since \mathbf{C} and \mathbf{D} are 3×3 cyclic matrices, it is evident that the matrices $\mathbf{C} + \mathbf{D}$ and $\mathbf{C} - \mathbf{D}$ are also 3×3 cyclic matrices. (Note that for a 6×6 cyclic matrix in Eq. (15), the powers of w in \mathbf{E} and \mathbf{F} in Eq. (16) are real numbers and imaginary numbers, respectively). In Eq. (16), \mathbf{E} is

$$\mathbf{E} = \begin{pmatrix} e_0 \\ e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} -0.445, & 1.247, & -1.802 \\ 1.247, & -1.802, & -0.445 \\ -1.802, & -0.445, & 1.247 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad (17)$$

where approximately $1/2 \operatorname{Re}(w^2 + w^5) = -0.445$, $1/2 \operatorname{Re}(w^1 + w^6) = 1.247$, etc. Let $a_0 = -1.802$, $a_1 = -0.445$, $a_2 = 1.247$ and $y_0 = 0$, $y_1 = 1$, $y_2 = 0$. Then the matrix equation defined in Eq. (17) can be obtained by computing the convolution of the two sequences a_n and y_n . This requires using a transform over $GF(q)$. To avoid overflow, one needs to choose $q = 7$ so that the integer components of a_n, y_n lie in the interval $\pm(7 - 1)/2$.

By Ref. 7, the sequence of a_n is converted first to a sequence of integers x_n in the dynamic range $A = 2$. Since 2 is a third root of unity, the transform over $GF(7)$ of x_n is

$$X_k = \sum_{n=0}^{3-1} x_n \cdot 2^{nk} = -1 + 2^{2k} \text{ for } k = 0, 1, 2$$

Thus $X_0 = 0, X_1 = 3, X_2 = 1$.

Similarly, the transform over $GF(q)$ of sequence y_n is

$$Y_k = \sum_{n=0}^{3-1} y_n \cdot 2^{nk} = 2^k \text{ for } k = 0, 1, 2$$

That is, $Y_0 = 1, Y_1 = 2, Y_2 = 4$. Define $E_k = X_k \cdot Y_k$, i.e., $E_0 = 0, E_1 = 6, E_2 = 4$. These are the only integer multiplications needed to perform this DFT. The inverse transform of E_k is

$$e_n = 3^{-1} \sum_{k=0}^{3-1} E_k \cdot 2^{-nk} \text{ for } n = 0, 1, 2$$

or

$$e_0 = 1, e_1 = -1, e_2 = 0$$

In a similar fashion, matrix F , given in Eq. (16), can also be obtained as $f_0 = -\hat{i}, f_1 = \hat{i} \cdot 0, f_2 = -\hat{i}$. Thus, by Eq. (16), one obtains $b_1 = 1/2 \hat{i}, b_2 = -1/2, b_3 = (1 - \hat{i})/2, b_4 = (1 + \hat{i})/2, b_5 = -1/2, b_6 = -\hat{i}/2$. Hence, finally $A_0 = 2 + \hat{i}0, A_1 = 1 + 1/2\hat{i}, A_2 = 1/2 + \hat{i}0, A_3 = 1/2(3 - \hat{i}), A_4 = 1/2(3 + \hat{i}), A_5 = 1/2 + \hat{i}0, A_6 = 1 - 1/2\hat{i}$. For this example, the dynamic range of $GF(7)$ is inadequate. Also there is a large truncation error due to the course approximation used for the roots of unity. Evidently, the DFT in this example has an accuracy of precisely two binary digits, including the sign bit. This example, though only illustrative, suggests that the large finite fields suggested above have more than adequate dynamic range to compute the DFT with small truncation error.

IV. Transforms of Very Long Sequences

To compute the DFT of much longer sequences than considered in the last section, let $d = d_1 \cdot d_2 \cdots d_r$, where $(d_i, d_j) = 1$ for $i \neq j$. By using the Chinese remainder theorem Ref. 18, it is shown by Winograd in Ref. 14 that the DFT matrix W can be transformed into the direct product of W_1, W_2, \dots, W_r , where W_i is the matrix of a d_i -point DFT. Assume the number of multiplications used to perform the d_i -point DFT for $i = 1, 2, \dots, r$ is m_i . Then, the number of multiplications for computing a d -point DFT is $N = m_1 \cdot m_2 \cdots m_r$. To illustrate this, see Winograd's example for computing a 12-point DFT, given in Ref. 15. By the same procedure used in the computation of this example, the number of integer multiplications needed to perform the transforms of longer sequences of complex numbers can be obtained by using Table 1 above and Table I in Ref. 14. These numbers are given in Table 2. The present algorithm and conventional FFT algorithm (Ref. 19) are compared in Table 2 by giving the number of real multiplications needed to perform these algorithms. The number of real multiplications needed to perform a transform of a few thousand points is given in Table II of Ref. 14.

Acknowledgements

The authors wish to thank Dr. N. A. Renzetti, Manager of Tracking and Data Acquisition Engineering, and the members of the Advanced Engineering Group in that organization at the Jet Propulsion Laboratory for their early support, suggestions, and encouragement of the research that led to this paper.

This work was supported in part by NASA Contract No. NAS 7-100, and also in part by the U.S. Air Force Office of Scientific Research under Grant AFOSR-75-2798.

References

1. Pollard, J. M., "The Fast Fourier Transform in a Finite Field," *Math. Comput.*, 1971, Vol. 25, pp. 365–374.
2. Schonhage, A., and Strassen, V., "Schnelle Multiplikation Grosser Zahlen," *Computing*, 1971, Vol. 7, pp. 281–292.
3. Rader, C. M., "Discrete Convolution via Mersenne Transforms," *IEEE Trans. Comp.*, 1972, Vol. C-21, pp. 1269–1273.
4. Agarwal, R. C., and Burrus, C. S., "Number Theoretic Transforms to Implement Fast Digital Convolution," *Proc. IEEE*, 1975, Vol. 63, pp. 550–560.
5. Agarwal, R. C., and Burrus, C. S., "Fast Convolution Using Fermat Number Transforms with Applications to Digital Filtering," *IEEE Trans. on Acoustics, Speech, and Signal Processing*, Vol. ASSP-22, No. 2, April 1974.
6. Reed, I. S., and Truong, T. K., "The Use of Finite Fields to Compute Convolution," *IEEE Trans.*, 1975, Vol. IT-21, pp. 208–213.
7. Reed, I. S., and Truong, T. K., "Complex Integer Convolution Over a Direct Sum of Galois Fields," *IEEE Trans.*, 1975, Vol. IT-21, pp. 657–661.
8. Vegh, E., and Leibowitz, L. M., "Fast Complex Convolution in Finite Rings," *IEEE Trans.*, 1976 Vol. ASSP-24, pp. 343–344.
9. Golomb, S. W., Reed, I. S., and Truong, T. K., "Integer Convolutions Over the Finite Field $GF(3 \cdot 2^n + 1)$," *SIAM J. on Applied Math.*, Vol. 32, No. 2, March 1977.
10. Pollard, J. M., "Implementation of Number-Theoretic Transforms," *Electro. Lett.*, 1976, Vol. 12, pp. 378–379.
11. Liu, K. Y., Reed, I. S., and Truong, T. K., "Fast Number-Theoretic Transforms for Digital Filtering," *Electron. Lett.*, 1976, Vol. 12, pp. 644–646.
12. Reed, I. S., Truong, T. K., and Liu, K. Y., "A New Fast Algorithm for Computing Complex Number-Theoretic Transforms," *Electron. Lett.*, 1977, pp. 278–280.
13. Reed, I. S., and Truong, T. K., "Fast Mersenne-Prime Transforms for Digital Filtering," to be published in *Proc. IEE*.
14. Winograd, S., "On Computing the Discrete Fourier Transform," *Proc. Nat. Acad. Sci. USA*, 1976, Vol 73, pp. 1005–1006.
15. Winograd, S., *On Computing the Discrete Fourier Transform*, Research Report, Mat. Science Dept., IBM Thomas J. Watson Research Center, Yorktown Heights, New York, 10592.
16. Agarwal, R. C., and Cooley, J. W., "New Algorithm for Digital Convolution," *IEEE Trans. Acoust., Speech, Signal Processing*, Vol. ASSP-25, pp. 392–410, Oct. 1977.
17. Reed, I. S., Kwoh, Y. S., Truong, T. K., and Hall, E. L., "X-Ray Reconstruction by Finite Field Transforms," *IEEE Transactions on Nuclear Science*, Vol. NS-24, No. 1, February 1977.
18. Niven, I., and Zuckerman, H. S., *An Introduction to the Theory of Numbers*, John Wiley and Sons, Inc., New York, 1966.
19. Cooley, J. W., and Tukey, J. W., "An Algorithm for the Machine Calculation of Complex Fourier Series," *Math. Comput.*, Vol. 19, pp. 297–301, April 1965.

Table 1. Complexity of hybrid DFT for real and complex data

$d = q'$	$q' - 1$	No. of integer multiplications for real data	No. of integer multiplications for complex data
367	$2 \cdot 3 \cdot 61$	488	976
373	$2^2 \cdot 3 \cdot 31$	620	1240
733	$2^2 \cdot 3 \cdot 61$	1220	2440
1831	$2 \cdot 3 \cdot 5 \cdot 61$	4880	9760
1861	$2^2 \cdot 3 \cdot 5 \cdot 31$	6200	12400
2441	$2^3 \cdot 5 \cdot 61$	8540	17080

Table 2. Complexity of new hybrid algorithm for DFT

d	Factors	New Algorithm No. of integer multiplications for complex data	Radix-2 FFT No. of real multiplications $2d \log_2 d$
4096	2^{12}		98,304
4476	$373 \times 4 \times 3$	14,880	
8192	2^{13}		212,992
8796	$733 \times 4 \times 3$	29,280	
16384	2^{14}		458,752
20888	$373 \times 8 \times 7$	89,280	
32768	2^{15}		983,040
41048	$733 \times 8 \times 7$	175,680	
62664	$373 \times 8 \times 7 \times 3$	267,840	
65536	2^{16}		2,097,152
123144	$733 \times 8 \times 7 \times 3$	527,040	
131072	2^{17}		4,456,448
262144	2^{18}		9,437,184
268560	$373 \times 16 \times 9 \times 5$	1,740,960	
524288	2^{19}		19,922,944
527760	$733 \times 16 \times 9 \times 5$	3,425,760	